SOPHOS



Sécuriser le Cloud public : 7 bonnes pratiques

Livre blanc Sophos Juin 2019

Sommaire

Sécuriser le Cloud public : 7 bonnes pratiques

Comment vérifier la sécurité de vos applications dans le Cloud public ? Parmi les réflexions ci-dessous laquelle vous donne confiance en vos applications hébergées dans le Cloud public ?

N'avoir pas été victime d'un vol de données cette année est-il suffisant ? Ou bien votre compréhension de l'infrastructure Cloud de votre entreprise suffit-elle à la protéger correctement ? Souhaitez-vous que vos audits de conformité se déroulent sans accroc ? Renforcer la collaboration entre vos équipes en charge de la conformité et du développement augmente-t-elle la sécurité et la mise en conformité ?

Quels que soient vos objectifs, ce guide peut vous aider. Il explore les 7 étapes clés pour sécuriser le Cloud public, à l'aide de conseils applicables à toute société. Il présente les résultats de recherche des SophosLabs sur la fréquence des attaques menées par les cybercriminels sur les instances basées dans le Cloud. Ce guide explore la manière dont Sophos Cloud Optix permet aux entreprises de répondre aux problèmes de sécurité et de visibilité.

Il est aisé de créer de nouvelles instances dans Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP). La difficulté pour les équipes en charge de l'exploitation, de la sécurité, du développement et de la conformité est de surveiller les modifications apportées aux données, aux ressources et à l'infrastructure dans ces environnements, afin que tout reste sécurisé.

Tandis que les fournisseurs de Cloud public sont responsables de la sécurité du Cloud (les datacenters physiques, ainsi que la séparation des environnements et des données des clients), vous êtes le seul responsable de la protection des ressources et des données placées dans le Cloud. Tout comme vous devez protéger les données stockées dans vos serveurs locaux, vous devez sécuriser votre environnement Cloud. La répartition des responsabilités est souvent mal comprise et cette confusion est exploitée par les pirates informatiques. Les ressources Cloud sont ainsi devenues leurs nouvelles mines d'or.

Les problèmes majeurs de la sécurité du Cloud

Étant donné la simplicité et le faible coût du Cloud public, il devient évident que les entreprises se tournent vers Amazon Web Services, Microsoft Azure et Google Cloud Platform. Il est aisé de créer une nouvelle instance en quelques minutes, d'augmenter ou de réduire les ressources selon les besoins, tout en ne payant que pour ce qui est utilisé et en évitant de payer des coûts élevés en matériel informatique.

Bien que le Cloud public élimine le besoin en matériel, il est cependant à l'origine de nouveaux casse-têtes. Le secret d'une cybersécurité efficace dans le Cloud est d'améliorer la sécurité globale : garantir la protection et la bonne configuration de votre architecture, obtenir la visibilité sur votre infrastructure, et, élément très important, sur ceux qui peuvent y accéder.

Sur le papier cela semble simple, mais la réalité est tout autre.

La progression rapide de l'utilisation du Cloud a fragmenté la répartition des données, avec des ressources dispersées dans plusieurs instances disparates et, pour certaines entreprises, plusieurs plateformes. Une entreprise moyenne utilise déjà 2 Cloud publics pour exécuter des applications, tout en expérimentant en parallèle 1,8 autre Cloud public [1]. Cette approche multi-Cloud pose un problème de visibilité aux équipes informatiques qui sont forcées de passer d'une plateforme à l'autre pour obtenir une image complète de leurs ressources dans le Cloud.

Le manque de visibilité sur les ressources basées dans le Cloud entraîne à la fois des risques de sécurité et de conformité :

Exposition accrue

Deux facteurs de motivation poussent les entreprises à migrer leurs ressources sur le Cloud : l'agilité et un meilleur délai de mise sur le marché des produits et des services. Pour cela, avoir recours à l'agilité et la réactivité de l'approche DevOps est impératif. Or cette nouvelle approche du développement et de la publication des versions de produits implique le travail de plusieurs développeurs sur de nombreuses plateformes, et aux fuseaux horaires différents.

Suivre les ressources ne posait pas de réel problème lorsque les cycles de développement duraient des mois, ou des années, mais cette époque est révolue. Vous devez tenir la cadence des nombreuses versions de produit, parfois même dans la même journée. Il est presque impossible de suivre 24 h/24 les modifications rapides de l'architecture, les mises à jour de configuration et les paramètres des groupes de sécurité. Cela se traduit par une exposition accrue aux cyber menaces, où les failles de sécurité peuvent être rapidement exploitées.

Risques pour les données, la propriété intellectuelle et les services

Le recourt au Cloud public est autant apprécié des entreprises que des cyber criminels. Les pirates d'aujourd'hui ciblent les serveurs Cloud en exploitant à leur profit les API natifs des fournisseurs de Cloud. Ils peuvent se déployer sur de nouvelles instances, violer des bases de données, changer des paramètres de sécurité et verrouiller les utilisateurs légitimes.

Pour avoir une meilleure idée de l'étendue du problème, les analystes des SophosLabs ont récemment configuré des environnements dans 10 des datacenters AWS les plus populaires au monde. Leurs recherches ont démontré que :

- En moins de 2 heures, l'intégralité des 10 serveurs Cloud a été victime de tentatives de connexion [2]
- Chaque serveur a subi en moyenne 13 tentatives d'attaque par minute, soit environ 757 par heure.

Ces résultats saisissants montrent la fréquence à laquelle les cybercriminels ciblent les instances dans le Cloud par des techniques sophistiquées et automatisées. Le défi pour les équipes de sécurité est d'identifier et de sécuriser les vulnérabilités potentielles avant qu'elles ne soient découvertes par les attaquants, et d'identifier en temps réel les comportements inhabituels (des attaquants) pour bloquer les attaques dès le départ.

Respecter la conformité aux normes

Peu importe où se situent votre infrastructure et vos données, vous devez démontrer que vous vous conformez aux normes applicables (notamment CIS, HIPPA, RGPD et PCI) à défaut, vous risquez des sanctions règlementaires.

La difficulté du Cloud est que les environnements changent de jour en jour, d'heure en heure, voire de minute en minute. Alors que les contrôles de conformité hebdomadaires ou mensuels étaient suffisants pour les réseaux locaux, ils ne le seront pas pour le Cloud public. La nécessité d'une analyse continue de la conformité peut représenter un énorme gaspillage de ressources pour les équipes qui gèrent les environnements de Cloud manuellement ou à l'aide d'outils natifs. Une fois qu'un problème de conformité est identifié, la dispersion des équipes de sécurité, de développement, d'exploitation et de conformité au sein des entreprises crée des difficultés de traitement en temps voulu.

Sept étapes pour sécuriser le Cloud public

Étape 1 : Comprenez vos responsabilités

Cela semble évident, mais la sécurité est gérée de manière un peu différente dans le Cloud. Les fournisseurs de Cloud public, comme Amazon Web Services, Microsoft Azure et Google Cloud Platform, utilisent un modèle de responsabilité partagée. Ils assurent la sécurité du Cloud, tandis que vous êtes responsables de tout ce qui est placé dans ce Cloud.

La protection physique des datacenters et la séparation virtuelle des données des clients et des environnements sont entièrement prises en charge par les fournisseurs de Cloud public.

Quelques règles de pare-feu basiques peuvent vous être octroyées pour gérer l'accès à votre environnement. Mais si vous ne les configurez pas correctement (par exemple si vous laissez des ports ouverts à tout vent), vous en serez le seul responsable. C'est pourquoi il est important de comprendre vos responsabilités en matière de sécurité.

La Fig. 1 vous offre un aperçu des responsabilités partagées. Vous pouvez également visionner une vidéo explicative ici.

Modèle de sécurité à responsabilité partagée	En local	Cloud public	Pourquoi ?
Utilisateurs	Client	Client	Appliquer l'authentification, définir des restrictions d'accès et surveiller l'utilisation des identifiants.
Données	Client	Client	Bloquer la perte des données, définir et mettre en application qui peut accéder à quelles données, tout en maintenant le respect des normes de conformité.
Applications	Client	Client	Empêcher la compromission d'une application par la mise en place de politiques, de correctifs et de mesures de sécurité.
Contrôles du réseau	Client	Client / Fournisseur de plateformes	Suivre et appliquer les autorisations d'accès au réseau.
Infrastructure de l'hôte	Client	Client / Fournisseur de plateformes	Gérer et protéger les systèmes d'exploitation, les solutions de stockage et les systèmes associés pour prévenir les bugs non corrigés et l'élévation de privilèges.
Sécurité physique	Client	Fournisseur de plateformes	Limiter l'accès physique aux systèmes et concevoir une redondance pour éviter la défaillance d'un point unique.

Client   Fournisseur de plateformes

Fig 1. Vue de Sophos sur le modèle de responsabilité partagée. Pour une version spécifique à chaque fournisseur de Cloud, visitez www.sophos.fr/public-cloud.

Étape 2 : Élaborez une stratégie multi-Cloud

Disposer de plusieurs environnements Cloud n'est plus une stratégie à privilégier. C'est au contraire devenu LA stratégie incontournable. Vous pourriez être amené à utiliser plusieurs environnements Cloud pour plusieurs raisons différentes : la disponibilité, plus d'adaptabilité ou certaines fonctionnalités particulières. Au moment de planifier votre stratégie de sécurité, partez du principe que vous utiliserez plusieurs serveurs Cloud différents. Si ce n'est le cas aujourd'hui, ce le sera sûrement dans un futur proche. De cette manière, vous pouvez pérenniser votre approche.

Pensez à la manière dont vous allez gérer la sécurité, la surveillance et la conformité de plusieurs serveurs Cloud, avec des systèmes et consoles séparés. Plus la gestion est simple, plus il est simple de diminuer le temps de réponse aux incidents, d'augmenter la détection des menaces et de réduire le casse-tête des audits de conformité. Sans parler d'une meilleure rétention de votre personnel qualifié.

Recherchez des solutions sans agent qui vous permettent de surveiller plusieurs environnements de Cloud depuis une seule console SaaS, de réduire le nombre d'outils, de personnels et de temps nécessaires pour gérer la sécurité sur un ensemble varié de comptes Cloud.

Étape 3 : Obtenez une visibilité complète

Vous ne pouvez pas sécuriser ce que vous ne voyez pas. C'est pourquoi l'un des principaux obstacles à l'adoption d'une bonne stratégie de sécurité est la visibilité complète sur votre infrastructure.

Tirez profit d'outils offrant la visualisation en temps réel de la topologie du réseau et du flux de trafic, avec un inventaire complet comprenant les hôtes, les réseaux, les comptes utilisateurs, les services de stockage, les conteneurs et les fonctions sans serveur.

Pour plus de visibilité, recherchez des outils capables d'identifier les éventuelles vulnérabilités au sein de votre architecture afin de prévenir tout point de rupture potentiel. Les zones de risques incluent :

- Les bases de données dotées de ports ouverts sur Internet qui pourraient permettre aux attaquants d'y accéder.
- Les services publics Amazon S3 Simple Storage Service.
- Les comportements de connexion et appels API suspects des utilisateurs, notamment les connexions multiples simultanées au même compte ou la connexion d'un utilisateur dans la même journée, mais depuis différents pays.

Étape 4 : Intégrez la conformité dans vos activités quotidiennes

En transférant vos ressources vers le Cloud vous devez respecter les règles de conformité sur un réseau plus distribué, ce qui implique souvent des versions de développement régulières. Pour garantir la conformité, vous devez créer un rapport d'inventaire précis et des diagrammes de réseau de l'empreinte de votre Cloud, et vous assurer que la liste de vérification de la conformité est respectée dans un environnement dynamique.

Lorsqu'il s'agit de respecter les délais d'audit, les entreprises se rabattent souvent sur la solution à court terme qui consiste à détourner des ressources de projets commerciaux rentables. Or, cette solution n'est pas viable à long terme et, comme les captures instantanées quotidiennes deviennent rapidement obsolètes, cela ne permet pas la surveillance continue de la conformité pour les normes telles qu'ISO 27001, HIPAA et RGPD.

Recherchez des solutions qui vous permettent d'améliorer votre conformité aux normes sans augmenter vos effectifs grâce à des captures en temps réel de la

topologie de votre réseau et à la détection automatique des modifications apportées à vos environnements de Cloud. Préférez également la possibilité de personnaliser les politiques de sécurité selon les besoins spécifiques de votre secteur.

Bien entendu, l'édition de rapport n'est qu'un aspect de la conformité. Vous devez également être en mesure de remédier aux problèmes de conformité. Le défi est bien souvent de réunir les bonnes personnes pour travailler ensemble entre les services d'exploitation, du développement et de la conformité en l'absence de voies de collaboration efficaces.

Pour faciliter la remédiation des problèmes de non-respect de la conformité, choisissez une solution qui s'intègre à votre système actuel de tickets informatiques, notamment des alertes pouvant être utilisées pour créer, assigner et suivre les problèmes jusqu'à leur résolution. De cette manière, les tâches importantes ne sont jamais perdues, même lors de la publication d'un produit.

Étape 5 : Automatisez vos contrôles de sécurité

La capacité à automatiser les processus est l'un des avantages de l'approche DevOps. Mais, tout comme vos équipes apprécient le déploiement automatisé de modèles et de scripts d'infrastructure, leur permettant d'économiser des heures de développement, vous devriez également réfléchir à automatiser certains contrôles de sécurité.

Dans le cadre collaboratif des pratiques DevOps, la sécurité est une responsabilité partagée, intégrée de bout en bout. Cette approche a été baptisée « DevSecOps », en mettant l'accent sur la nécessité de créer des bases de sécurité solides pour les initiatives de DevOps.

Automatiser la sécurité est devenu un réel enjeu, car les cybercriminels utilisent eux-mêmes de plus en plus l'automatisation pour mener leurs attaques. Ils utilisent par exemple des identifiants utilisateur volés pour automatiser le provisionnement d'instances afin d'y réaliser des activités frauduleuses telles que le cryptojacking, la modification des paramètres du compte ou la révocation des utilisateurs légitimes pour éviter d'être détectés. En effet, il est désormais monnaie courante que les environnements de Cloud soient ciblés à la recherche de failles de sécurité dans les mots de passe, les paramètres de groupes de sécurité ou le code.

Deux raisons principales expliquent pourquoi certains environnements de Cloud publics ne peuvent pas lutter contre ces attaques : la configuration de l'architecture n'est pas sécurisée et la réponse aux menaces n'est pas aussi performante que les attaques. L'automatisation des contrôles de sécurité est essentielle pour faire face à ces problèmes.

Pour garantir la sécurité de vos environnements de Cloud publics, intéressez-vous aux solutions qui offrent :

- **Remédiation automatique des vulnérabilités de l'accès utilisateur et des ressources**, avec entrée depuis n'importe quelle source sur n'importe quel port.
- **Identification des événements de connexion à la console et des appels API suspects** qui suggèrent l'utilisation par un attaquant d'identifiants utilisateur partagés ou volés.
- **Signalement des anomalies du trafic sortant** pour alerter votre entreprise des activités frauduleuses telles que le cryptojacking ou l'exfiltration de données.
- **Identification de charges de travail d'applications cachées** à partir du comportement de l'instance sur l'ordinateur hôte afin de mettre au jour les points d'exposition cachés (par ex. les bases de données).

Étape 6 : Sécurisez TOUS vos environnements (y compris Dev et QA)

Bien que les cas récents d'attaque sur des Cloud publics l'ont été sur les environnements de production des entreprises (ceux utilisés par vos clients), les attaquants sont tous autant susceptibles de cibler votre capacité informatique, c'est-à-dire vos environnements de développement et d'analyse qualité, pour du cryptojacking par exemple.

Vous avez besoin d'une solution qui puisse sécuriser tous vos environnements (PROD, DEV et QA) de manière réactive, mais aussi proactive. La solution doit pouvoir traiter tous vos journaux d'activités (logs de flux VPC, logs CloudTrail, etc.) pour identifier les incidents qui se sont déjà produits, par exemple lorsqu'un port non désiré est ouvert dans le pare-feu. En parallèle, la solution devrait être capable d'analyser de manière proactive les modèles d'infrastructure programmable (IaC) de vos répertoires, tels que GitHub, et de les intégrer à vos outils de pipeline CI/CD, tels que Jenkins. Ainsi, les vulnérabilités introduites dans le code sont détectées bien avant que ce dernier ne soit déployé sur vos serveurs, vous évitant ainsi de faire les prochains gros titres des journaux.

Étape 7 : Réemployez les pratiques de sécurité que vous utilisez déjà en local

Ce conseil peut sembler surprenant dans un guide sur le Cloud public, mais la sécurité de votre infrastructure locale est le résultat de décennies d'expérience et de recherche. Lorsqu'il s'agit de protéger vos serveurs Cloud contre les infections et les pertes de données, commencez par réfléchir à ce que vous faites déjà pour votre infrastructure traditionnelle et adaptez-la pour le Cloud :

- Pare-feu Next-Gen : Empêchez les menaces d'atteindre vos serveurs Cloud en utilisant un pare-feu pour applications Web (WAF) au niveau de votre passerelle Cloud. Pensez également à inclure un IPS (Intrusion Prevention System) (pour faciliter la conformité) et le contrôle du contenu sortant pour protéger vos serveurs/VDI.
- Protection des serveurs : Appliquez une cyber protection efficace à vos serveurs Cloud, tout comme vous le feriez sur vos serveurs physiques.
- Protection des terminaux : Bien que votre réseau soit dans le Cloud, vos ordinateurs portables et autres périphériques restent au sol, et il suffit d'un email de phishing ou d'un spyware pour voler des identifiants utilisateur de vos comptes Cloud. Assurez-vous de bien mettre à jour la sécurité de vos terminaux et de vos messageries sur tous vos appareils afin de prévenir tout accès non autorisé aux comptes Cloud.

Présentation de Sophos Cloud Optix :

Visibilité complète, protection intégrale

La visibilité est le fondement sur lequel toutes les politiques de sécurité et les activités du Cloud public se basent. Sophos Cloud Optix simplifie la surveillance de plusieurs environnements de Cloud, dont Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), clusters Kubernetes et répertoires de code de développement. Cette visibilité supérieure, associée aux alertes et aux contrôles de politiques de conformité et DevSecOps, permet aux équipes de prendre le contrôle et de renforcer leur stratégie de sécurité Cloud en toute confiance.

Cloud Optix est un service SaaS sans agent qui s'intègre avec les API natifs du fournisseur de Cloud public. Cela permet de construire automatiquement une image complète de l'architecture de Cloud, dont un inventaire complet et une visualisation en temps réel de la topologie du réseau comprenant hôtes, réseaux, comptes utilisateurs, services de stockage, conteneurs et fonctions sans serveur.

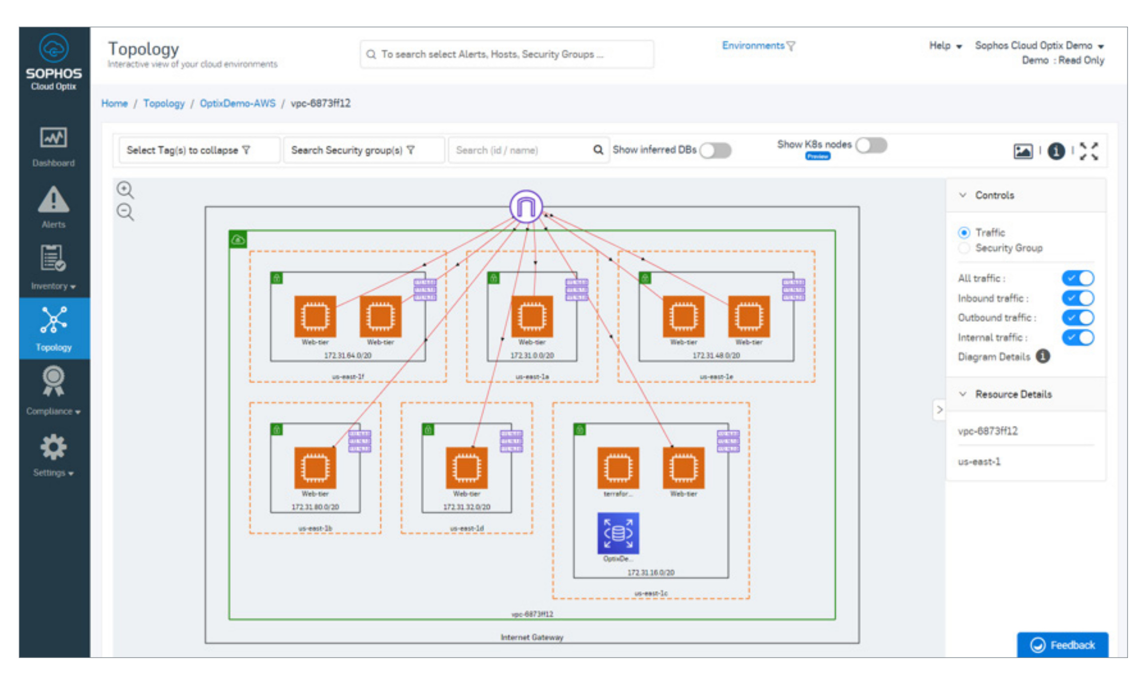


Fig 2. La visualisation de la topologie du réseau de Sophos Cloud Optix montrant le trafic entrant, sortant et interne au sein d'un environnement AWS.

Bien plus que de simples contrôles de la configuration

Cloud Optix utilise l'intelligence artificielle du Machine Learning pour détecter les anomalies et les failles de sécurité sur l'ensemble de votre plateforme. Il surveille le trafic réseau, la configuration des ressources, les événements de connexion des utilisateurs et des appels API, l'état de la conformité, les répertoires d'infrastructure programmable (IaaC) et bien plus encore. Il est doté de garde-fous permettant de prendre automatiquement les mesures nécessaires si des modifications accidentelles ou frauduleuses de la configuration du réseau sont détectées.

En parallèle, les alertes contextuelles identifient l'origine des problèmes de sécurité et de conformité, vous permettant de vous concentrer sur les zones les plus critiques nécessitant des mises à jour de sécurité. Les alertes affichent une description du problème, les étapes à suivre et les ressources affectées.

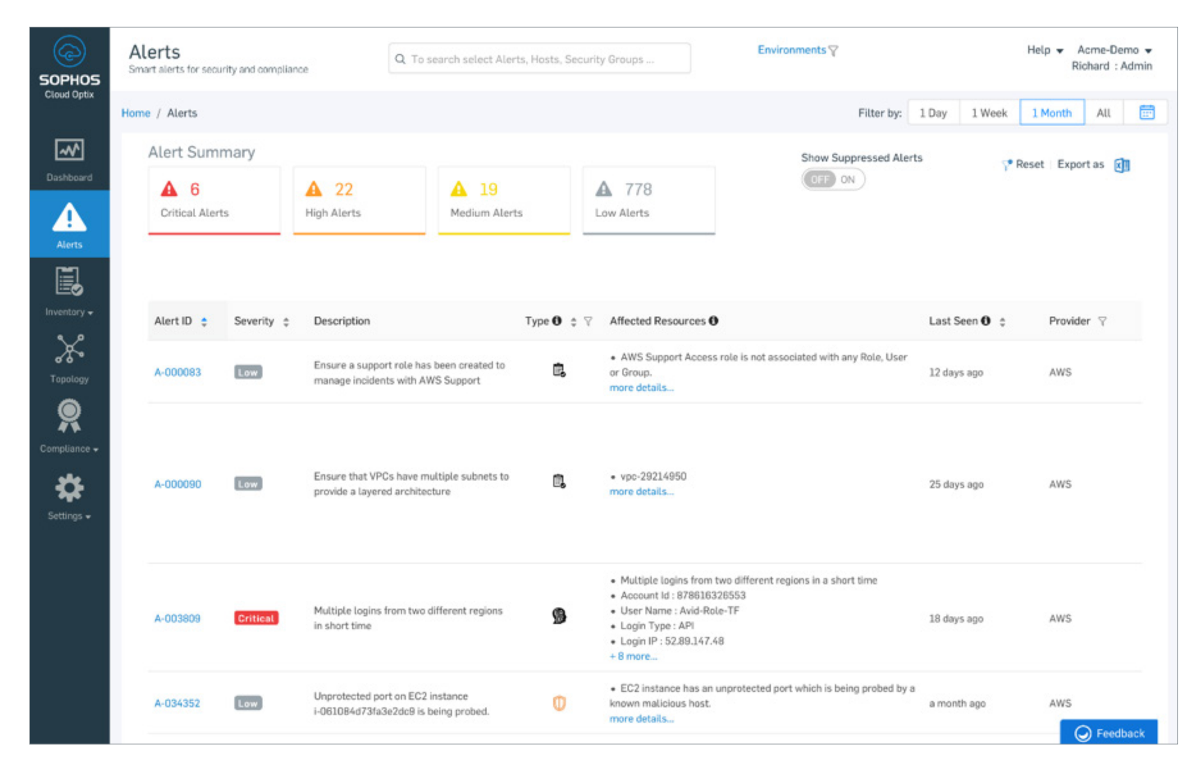


Fig 3. L'onglet « Informations sur les alertes » de Sophos Cloud Optix affiche une alerte critique liée à la connexion simultanée d'un utilisateur depuis deux pays différents.

Surveillez et répondez à votre manière

Cloud Optix fournit une API REST et s'intègre avec Splunk, PagerDuty et Amazon GuardDuty pour vous fournir en temps réel des informations sur les alertes partout où vous en avez besoin. Grâce à l'intégration embarquée avec Jira et ServiceNow, les informations sur les alertes peuvent même être utilisées pour créer des tickets qui peuvent ensuite être suivis jusqu'à leur résolution. De cette manière, les tâches importantes ne sont jamais perdues, même lors de la publication d'un produit.

Les alertes sont affichées dans un rapport consultable à la demande depuis un seul écran dans le tableau de bord, vous permettant d'économiser un temps précieux dans la gestion de votre stratégie de sécurité Cloud. Vous n'aurez alors aucun mal à suivre les 7 étapes essentielles pour sécuriser le Cloud public.

En savoir plus

Sophos Cloud Optix est la solution idéale pour les entreprises qui utilisent ou qui souhaitent migrer leurs ressources vers le Cloud public. En associant la puissance de l'intelligence artificielle à l'automatisation, votre entreprise dispose de la visibilité continue nécessaire pour détecter, répondre et prévenir les failles de sécurité et de conformité qui pourraient vous mettre en danger.

Pour en savoir plus sur Sophos Cloud Optix et pour démarrer un essai gratuit sans obligation sur vos propres environnements Cloud, ou pour une démonstration en ligne immédiate, visitez www.sophos.fr/cloud-optix.

Conclusion

Passer de ressources traditionnelles à des ressources Cloud offre des avantages substantiels aux entreprises de toutes tailles. Cependant, il est impératif de sécuriser le Cloud public afin de protéger votre infrastructure et votre entreprise contre les cyberattaques. En suivant les 7 étapes de ce guide, vous optimiserez la sécurité de vos Clouds publics tout en simplifiant la gestion de la sécurité et l'édition de rapport de conformité.

Modèle de responsabilité partagée : Sophos peut vous aider

	En local	Cloud public	Pourquoi ?	Sophos assiste
Utilisateurs	Client	Client	Appliquer l'authentification, définir des restrictions d'accès et surveiller l'utilisation des identifiants.	XG Firewall et Sophos UTM mettent en œuvre l'authentification entrante et sortante avec l'authentification unique (SSO) et l'authentification à deux facteurs (2FA) et créent des rapports détaillés sur les accès. Sophos Cloud Optix surveille l'utilisation partagée ou non autorisée des identifiants d'un compte utilisateur.
Données	Client	Client	Bloquer la perte des données, définir et mettre en application qui peut accéder à quelles données, tout en maintenant le respect des normes de conformité.	Sophos Cloud Optix automatise la conformité, le respect de la gouvernance et du suivi de la sécurité dans le Cloud, tandis que Sophos SafeGuard, la DLP et Sophos Mobile sécurisent les données et déterminent les droits d'accès.
Applications	Client	Client	Empêcher la compromission d'une application par la mise en place de politiques, de correctifs et de mesures de sécurité.	Les fonctions IPS de XG Firewall et Sophos UTM et HIPS + verrouillage de Server Protection protègent contre les attaques et l'exposition involontaire des applications.
Contrôles du réseau	Client	Client / Fournisseur de plateformes	Suivre et appliquer les autorisations d'accès au réseau.	L'interface simple de XG Firewall et de Sophos UTM, ainsi que l'inspection puissante des paquets et la sécurité synchronisée (XG uniquement) aident à protéger et à gérer l'accès au réseau et à appliquer les privilèges réseau.
Infrastructure de l'hôte	Client	Client / Fournisseur de plateformes	Gérer et protéger les systèmes d'exploitation, les solutions de stockage et les systèmes associés pour prévenir les bugs non corrigés et l'élévation de privilèges.	Sophos Intercept X protège contre les menaces Zero-Day en se concentrant sur les techniques d'exploit. La fonction de verrouillage de Sophos Server Protection applique les restrictions d'exécution et Sophos XG Sandstorm bloque la prolifération de code inconnu.
Sécurité physique	Client	Fournisseur de plateformes	Limiter l'accès physique aux systèmes et concevoir une redondance pour éviter la défaillance d'un point unique.	XG Firewall et Sophos UTM ont tous deux des options de déploiement en haute disponibilité pour les pare-feu physiques et pour les plateformes Cloud.

Client — Fournisseur de plateformes

Fig 4. Sophos peut vous aider avec le modèle de responsabilité partagée du Cloud public.

« Sophos Cloud Optix apporte à notre équipe une visibilité intelligente et en temps réel sur nos environnements AWS et sur l'état de conformité de notre configuration. Cela permet un niveau de surveillance et d'alerte qui était auparavant impossible sur une seule console. Avoir Sophos Cloud Optix nous donne une vision globale de l'activité de l'infrastructure, et nous permet de nous concentrer sur des protections complètes. »

Ryan Stinson
Manager of Security Engineering
HubSpot Inc.

1 RightScale 2019 State of the Cloud Report de Flexera

2 Automated attack data source: Exposed: Cyberattacks on Cloud Honeypots, Matt Boddy, Sophos, Avril 2019

Testez Sophos Cloud Optix

www.sophos.fr/cloud-optix

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

19-06-19 WP-FR (RP)

SOPHOS